The following Listing of Claims will replace all prior versions, and listings, of claims in the present application:

Listing of Claims:

1. (Currently amended) A method for protected execution of a cryptographic calculation, in which a key ~~(12)~~ with at least two key parameters ~~(p, q, pinv, sp, dp, sq, dq)~~ is drawn on, wherein an integrity check ~~(30, 34, 40, 54)~~ of the key ~~(12)~~ is performed ~~in the method,~~ in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter ~~(p, q, pinv, sp, dp, sq, dq)~~ by corrupting at least one first key parameter ~~(p, q, pinv, sp, dp, sq, dq), characterized in that at least one key parameter (dp, dq) is the product of a value required for the cryptographic calculation times a safeguard value (sp, sq), and in that the integrity check (30, 34, 40, 54) includes a divisibility check~~.

2-13. Canceled.

14. (New) A method as claimed in claim 1, wherein in the integrity check it is determined whether the value of at least one key parameter is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps.

15. (New) A method as claimed in claim 1, wherein in the integrity check it is determined whether at least two key parameters are in a predetermined relationship to one another.

16. (New) A method as claimed in claim 1, wherein the integrity check includes a multiplicative operation, in particular a divisibility test.

17. (New) A method as claimed in claim 1, wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by the safeguard value.

18. (New) A method as claimed in claim 1, wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value.

19. (New) A method as claimed in claim 1, wherein in the integrity check a checksum stored with the key parameters is compared with a checksum newly calculated after passing of the key parameters.

20. (New) A method as claimed in claim 1, wherein, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing.

21. (New) A method as claimed in claim 1 , wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method.

22. (New) A method as claimed in claim 21, wherein the RSA method is an RSA-CRT method.

23. (New) A method as claimed in claim 21, wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value.

24. (New) A method as claimed in claim 23, wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying.

25. (New) A method as claimed in claim 21, wherein the prime factors of the RSA method are multiplied by a masking parameter and the error freedom of the calculation sequence is checked by an equality check modulo the masking parameter.

26. (New) A method as claimed in claim 1, wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

27. (New) A method for determining a key for a cryptographic calculation with at least two key parameters, the key being adapted to be used in a method for protected execution of a cryptographic calculation wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are

drawn as to at least one second key parameter by corrupting at least one first key parameter.

28. (New) A method as claimed in claim 27, characterized in that at least one key parameter is obtained by multiplication of a value required for the cryptographic calculation by a safeguard value.

29. (New) A method as claimed in claim 27, wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

30. (New) A computer program product which has program commands to cause a processor to execute a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

31. (New) A computer program product as claimed in claim 30, wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

32. (New) A portable data carrier set up for executing a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

33. (New) A portable data carrier as claimed in claim 32, wherein the data carrier is one of a smart card and a chip module.

34. (New) A portable data carrier as claimed in claim 32, wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.